COMPUTERWORLD®

Peer Perspective. IT Leadership. Business Results. | COMPUTERWORLD.COM | JULY 18, 2011

Should CIOs Have a Foreign Policy?

Businesses need contingency plans for political uprisings, terrorist attacks and natural disasters around the world.

» International SOS executives Michael Shea (left) and Jonathan Bar activate a business continuity plan every three to four weeks.

Should CIOs Have a Foreign Policy?

BY MINDA ZETLIN

With business operations entangled in the unpredictable and sometimes volatile global scene, **the answer is a resounding 'yes'** *(and the more detailed, the better).*

IN JULY 2005, a series of suicide bomb attacks in London's transit system killed 56 people and threw the city into a state of confusion. The U.S.-based CEO of a multinational financial company with offices in London posed what to him seemed a simple and essential question: "Are all our people OK?"

Getting an answer proved challenging. First, there was no single staff directory that covered the entire company and was kept up to date with ongoing staff changes. Nor was there a single directory of every person's location and contact information. Second, even if it existed, such a directory would not have included contractors, who nonetheless fit within the CEO's definition of "our people."

Third, there was no central record of which London employees were on vacation, on leave or traveling that day, or — more worrisome — which employees from other locations might be visiting London. And finally, even for those employees who were known to be in London and for whom the company had addresses and phone numbers, it was hard to make contact.

DOMINIC EPISCOPO

When Did You Last Practice Your Plan?

ONCE YOU ADOPT an effective business continuity plan, the worst thing you can do with it is … nothing. But too many companies do just that. With well-thought-out business continuity and disaster recovery plans in place, they assume they're prepared for whatever comes along.

There are two problems with that. First, people tend to forget what they don't rehearse. And second, the constant pace of technological and business changes will render almost any plan useless within a couple of years if you don't frequently update it.

"Whatever you decided to do two years ago – do you still have the appropriate levels of technology to make it happen?" asks Terry Assink, group vice president at Brand Velocity. "Have you changed things, upgraded things or moved functions elsewhere such that your plan isn't valid anymore?" Many organizations today have a model that's different from what they once had, with fewer functions and less data on-site and more data residing in the cloud. The effect is that a local crisis that interrupts communications and/or power will pose a different set of problems than it would have in the past.

In particular, Assink notes, the importance of maintaining an Internet connection has grown dramatically in the recent past. "We used to think about the internal network and the outside network, and the outside one had a secondary role," he says. "Now, they each have the same level of importance. A lot of the collaboration that goes on between employees and with partners and customers is conducted over the Internet today."

In addition to reviewing your business continuity plan at least once a year, you should also practice it at least as often. Communications provider Orange Business Services engages in unannounced audits to test business continuity plans at each of its support centers. The company conducted just such a test at its Cairo location about a week before the Egyptian uprising started, curfews were imposed, and the government cut off SMS and Internet communications. With a well-rehearsed plan in place, Orange was able to swiftly move disrupted support functions to its other centers in India, Brazil and Mauritius, and then smoothly return them to Cairo nine days later, after the Internet was restored and relative calm had returned.

International SOS practices its business continuity and disaster recovery plans at each of its 70 worldwide locations at least once every six months, according to Michael Shea, executive vice president for IT. "One thing we realized when we first started doing this is that the first time we practice something, we are horrible at it," he says. "When we go to set up a data center at a disaster recovery site, whether hot, warm or cold, it never goes well the first time. We need at least two practices to do it smoothly. So if we practice once every six months, it takes us at least a year to get good at it."

– MINDA ZETLIN

"Transportation was disrupted, cellphone service was down, SMS was down, and it was very unclear for most of the day just what had happened," recalls Andrew Marshall, director of Consultifi, which helps companies understand business risks.

The company's HR and IT departments weren't able to provide a timely answer to the CEO's questions, he says. "It turned into a conversation that involved philosophy and technology as well as HR," Marshall notes.

There are several lessons any IT leader can draw from this tale. First, there's no such thing as a safe location: Disruptions can happen anywhere. Second, it's important to have a plan that spells out what everyone's responsibilities will be and includes all the information you'll need. And finally, you need redundant communications systems, because "normal" methods of communication will likely fail — especially mobile, which is quickly overwhelmed by the spike in local demand that takes place during any crisis.

Concerns About Crisis Events Grow

It would be impossible to think about events of the past 12 months without having at least a few qualms over systems, data and employees, especially those outside the U.S., and the possible effect of local unrest, epidemics, earthquakes or other hazards. Indeed, in a 2010 survey of the 100 largest technology companies, 55% of executives reported worrying about "natural disasters, war, conflicts and terrorist attacks." When the same executives were again asked that question in 2011, that percentage rose to 81%.

In this increasingly global and interconnected world, it's easy to see why they're concerned. Power outages, weather events, political unrest or even something as mundane as a ship dragging its anchor over a fiber-optic cable can disrupt your operations in unexpected ways. Data centers could go offline. Data stored in remote locations could become unavailable, as could your supply chain. You could lose contact with offshore service providers due to interrupted communications. Software-as-a-service applications could go offline. And although cloud-based infrastructure is mostly hosted in the U.S. now, that's expected to change in the next few years, posing even greater risks.

In fact, a significantly global operation is likely to be affected by local disruptions — somewhere — on a very regular basis.

"There are events happening almost constantly at any time in different parts of the world, whether a bombing in Jakarta or an uprising in Egypt or an earthquake in Japan," says Michael Shea, executive vice president for IT at International SOS, a company that provides medical and security services to travelers and has operations in 70 countries. With so many locations — many of them in emerging markets and other politically or economically unstable areas — operating through a crisis is business as usual. "We have to activate one of our business continuity plans about every three to four weeks," Shea says.

> **Crisis management isn't just a function of senior or midlevel management.** It needs to be known and understood by everyone.
>
> **JONATHAN BAR,** GENERAL MANAGER OF GLOBAL INFRASTRUCTURE, INTERNATIONAL SOS

Even if you have few operations in unstable areas, it's wise to consider what events could disrupt your overseas operations, affect your overseas data or threaten your overseas employees. A well-thought-out foreign policy should be part of every CIO's toolkit. But how can you effectively prepare for whatever disasters the world might throw at you? Here are some ideas that might help.

Don't Plan for Everything Everywhere

In omnia paratus —"Ready for anything!" This might seem like a good approach to protecting your IT operations from all perils overseas. And indeed, some IT leaders take the position that, since there's no way to predict what might happen next in any geographic location, the best strategy is to be ready to meet absolutely any threat anywhere it may arise.

There's only one problem with this approach: It's impossible to do. "Trying to prepare for everything everywhere leads you down one of two paths, neither of which is good," says Dan Blum, an analyst at Gartner. "One path is saying that whatever you're doing will have to be good enough, since you can't know everything. The other is the path of being too paranoid and exhausting yourself chasing phantoms, and no organization can do that for very long. CIOs or chief information security officers who attempt to create and maintain the same very high level of preparedness everywhere will find their credibility eroding and their influence declining over time."

On the other hand, it can be very hard to see even a short distance into the future. Consider Orange Business Services, the business communication arm of one of Europe's largest mobile providers. The company has four major support centers in Egypt. One day last winter, Paul Joyce, senior vice president of international customer service and operations, paid a routine site visit to the company's facility near Cairo. With protests sweeping through nearby Tunisia, Joyce asked the company's local staffers whether they anticipated civil unrest in Egypt as well.

"They joked that the worst trouble would arise from [ousted president] Ben Ali flying by overhead on his way to Paris," Joyce says. "They were sure it would never happen there." Only a week later, they were proved wrong.

You can't be ready for everything everywhere, but at the same time, specific events in specific places can be nearly impossible to foresee. So how do you prepare?

"My recommendation is a balancing act," Blum says. "You want to raise your baseline capability to cope with any crisis. You raise that as high as you reasonably can, given the costs and potential benefits. But then you look at worst-case scenarios that would be catastrophic to the business in terms of what's most likely to happen, and that will vary by location." (For more on how to calculate the risk of specific events in different places, see "How to Create a Valid Threat Matrix" below.)

Should you watch the news with special attention to potential disasters brewing where your data, operations or outsourcing partners are located? "Anyone with access to the Internet and a news service should have a basic idea of what's going on," Marshall says. But, he adds, you shouldn't try to go it alone. "Every organization needs to monitor external events. You may have a risk management team within your company, or there are commercial organizations that will keep you updated about potential risks."

One of your best sources of information is whatever staff you have on the ground in a potentially troubled location. Depend on them for insight, and make sure they have a plan for where to get their own news if a local event causes disruptions.

Sometimes it's possible to see a problem coming well in advance. Although the earthquake and damaged nuclear reactor in Fukushima, Japan, are no longer making daily headlines, Orange is helping a client located nearby consolidate and relocate operations to Indonesia as soon as possible. Why? "The biggest challenge for many there was power continuity," Joyce says. "Coming into the peak of the summer, there will still be a serious aftereffect of that disaster. We're anticipating rolling blackouts."

Ask 'What if?'

Once you've considered what types of disruptions are most likely at your various locations, sit down with key staffers and talk through each of those scenarios.

"It's worth running through a catalog that might include civil unrest, power supply problems, interruption of Internet service and a terrorist attack, although trying to imagine and

How to Create A Valid Threat Matrix

In South Africa, phone lines often fail because people desperate for money pull them apart to sell the copper wire. In the Philippines, electrical fires are a frequent problem. There's no doubt that knowing the likelihood of a particular threat in a particular location is key to business continuity planning. But is there a useful way to take all the various factors into account?

International SOS, which provides medical and security services to travelers in 70 countries, comes as close as humanly possible by creating a specific risk matrix for every one of its locations. "We look at about 50 different categories of events, and for each we rate the possibility of it happening from 1 to 5," explains Jonathan Bar, general manager of global infrastructure.

IT executives obtain this information by working directly with local employees. They're asked how many times a given event has taken place in their location during the previous year, five years, 10 years and 100 years. Once you take such a long view, some recent startling events become slightly less surprising. "You'd have to go back to the 1970s and the presidency of Anwar Sadat, but there was rioting in Egypt then," Bar says. "That was only about 30 years ago, so it could happen again."

Once you have a threat matrix established for a particular location, it's easier to plan for the likeliest disruptions. In Thailand, for instance, depending on how you count, there have been 20 attempted or successful coups in the past 100 years. During the most recent attempt, the local International SOS office was surrounded by tanks.

"So we adjust our planning for Thailand with the view that the odds of civil unrest are very high," Bar says. "When it comes to tornadoes there, we're not overly concerned."

— MINDA ZETLIN

foresee everything will take you down some blind alleys," Marshall says.

It's an important opportunity to learn just what top management will expect of IT in a crisis. "See if everyone's assumptions are the same," Marshall suggests. "Ninety percent of the time, someone will say, 'I thought you guys would be up and running for that!' "

People tend to assume that working systems stay that way, he notes. "Anyone who's worked in a company with centralized data storage knows there are all kinds of misconceptions about what you will and won't be able to access, and the assumptions you make in IT won't be the same ones that Finance or other departments make." Key areas to cover for each scenario: Will the Internet be available? What about phone service? If data needs to be restored from a backup, how long will it take? "People tend to assume that, since we have backups, the data will be instantaneously available," Marshall says.

Another reason for this exercise is for you to learn which systems are most essential to keeping the company running — and they may not be the most complex or challenging ones from IT's point of view. "Generally, anything around your revenue stream is highly critical," says Terry Assink, group vice president for Brand Velocity, which consults on business project implementations, and former CIO of Kimberly-Clark. "You need to be able to take in money, and you need to be able to pay your employees."

"Your finance department may be very needed during a crisis," adds Shea. "If you're in Egypt during the unrest, and you need to charter airplanes so you can get people out of there safely, you will need finance people and financial resources to make that happen."

Asking "What if?" made a huge difference for Allied Telesis, which supplies communications for the U.S. Air Force base in Yokota, Japan, about 190 miles from Fukushima, where much of the local infrastructure was destroyed. Despite massive problems and power outages, the Yokota base never lost communications.

One reason is that less than three weeks before the Fukushima earthquake, a huge earthquake struck Christchurch, New Zealand. "That earthquake did spur us to look at certain elements of our operation in Japan," notes Keith Southard, CEO of Allied Telesis. "As a result, we completed a key power project in our network at Yokota Air Base just days before the earthquake there. Had we not completed the project before the earthquake, our operations during the crisis would have been much more difficult. A key lesson from this is to not just be aware of what has occurred elsewhere, but then to overlay that event on your own systems and operations and evaluate where you can improve those systems."

Another benefit of asking "What if?" is that it may help you make (or influence) better decisions about where to locate critical data or IT operations in the first place. As a corporate CIO, Southard says, "you should have some input to the business as to the importance of a given location and the risks there."

Think Militarily

Ever notice that soldiers, police officers and emergency responders often appear to remain calm in the middle of a crisis? That's because they know they have a specific set of rules and procedures to follow, which allows them to stay focused and keeps them from panicking while trying to figure out what to do next. Take a page from their playbook and create an equally well-laid-out set of plans and procedures for your staff to follow in a crisis situation.

With locations in 70 countries and crisis plans activated on a monthly basis, International SOS takes this approach. Its IT team has gotten adept at creating plans that are extremely detailed. Most come not only with very specific tasks and responsibilities that each employee must take on in a crisis, but even a diagram of where each team member will sit in the crisis management room. The information is reinforced with rehearsals. And there are diagrams and posters at company locations, reminding employees where to go during a crisis, or that they should notify a supervisor if one of their special internal phone lines rings.

"You have to make it dummy-proof," Shea explains. "In an incident like the Japanese earthquake, everyone is shocked. No one is prepared for something like that, and they need to have very clear guidance."

That goes for people far from the crisis location as well. One important but often forgotten task is to get word out to the rest of your organization, and perhaps your customers as well, letting them know that you have the crisis in hand, and whether and how it may affect them. When rioting and the Internet suspension in Cairo caused Orange Business Services to temporarily suspend operations at its support center there, the company set up an internal Microsoft SharePoint site where its employees could check for status updates and find answers to frequently asked questions. "It got more than 3,000 hits a day," Joyce notes. "That was a lot more efficient than having to send out emails or set up conference calls." Indeed, you might

What's in Your Crisis Suitcase?

When a crisis strikes at an International SOS location, local employees pull out the field deployment pack. That's a suitcase full of technology items that are especially useful when normal power and/or communications are down. It's a good idea to have a similar bag of tricks stored in a closet at each of your company's locations.

Here are the contents of an International SOS field deployment pack:

- **Several laptops**
- **Satellite phones**
- **A satellite Wi-Fi hotspot**
- **A mobile printer**

The printer is more important than you might think, explains Jonathan Bar, general manager of global infrastructure. You may need to print travel papers or other documents, or photos of people you're searching for.

Recently, the company has begun including iPads in its field deployment packs. With their high-quality image display capability, long battery life and robust mapping technology, they can be very handy.

– MINDA ZETLIN

consider having a template website set up so it's ready to go when a crisis occurs.

When planning for a crisis, in addition to using posters and diagrams, International SOS IT execs have frequent meetings with employees in various locations to map out who will do what. "We look at each individual department and break it down into action plans," says Jonathan Bar, general manager of global infrastructure. "They're like flowcharts for each department to follow that the supervisor leading the charge can refer to. They lay out particular steps, with information and contact numbers to call, so they can activate the plan. It walks them through all the steps."

Keep in mind that in an emergency, all employees can be called on to help out, not just those with IT or support jobs. "We may have someone who works in finance, on collections," Bar says. "In the middle of a crisis, we aren't collecting from our customers, but that person is still valuable because he or she can step in and take over a role where someone else is exhausted, such as answering phones."

Likewise, he says, it's important to include all employees in crisis planning meetings. "Crisis management isn't just a function of senior or midlevel management. It needs to be known and understood by everyone," Bar says.

"The real key is to understand the value of your people," he adds. "They're your most important asset, and they can keep you moving forward." ◆

Zetlin *is a business technology writer and co-author of* The Geek Gap: Why Business and Technology Professionals Don't Understand Each Other and Why They Need Each Other to Survive.